IT STD-010

Office of Information Technology Standard

Security: Authentication / Biometrics

Definition(s):
Biometrics refers to technologies for measuring and analyzing human body characteristics especially for authentication purposes.

Biometric authentication methods are:

- Finger scan (fingerprints)
- Hand geometry
- Iris and retina scans
- Facial scans
- Voice recognition

Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and a database that stores the biometric data for comparison with master or template records. When converting the biometric input, the software identifies specific points of data as match points. The match points from the scanned area are compared to the match points on file when a user tries to gain access.

Rationale:
Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is necessary. Biometric-based solutions augment passwords or PINS, to provide a more secure method of authentication.

Approved Standards:

- Biometric authentication systems deployed must meet accepted industry standards in order to maximize long term cost effectiveness and for ease of integration.   Accepted file formats are:
    - HA-API
    - Bio-API
    - CBEFF
- Speech applications must comply with the SAPI standard for speech recognition.
- Biometric authentication systems must also comply with additional standards as developed by the MI Technical Committee.
- Biometric authentication software must be integrated to use Microsoft Active Directory as the repository for biometric credentials. However, this does not preclude storing a copy of the biometric credentials at the user level.

Approved Products:
To be determined. The Office of Information Technology (OIT) intends to establish product standards and master contracts to take advantage of volume pricing for the statewide enterprise.

Guidelines/Technical Considerations:
Biometric authentication systems are not mandatory. IT-POL-006 states agencies must use at least one method of authentication. Biometric authentication systems may be combined with other authentication methods to create higher levels of security or as a backup, in the event of failures in the biometric authentication process. All primary and secondary authentication methods must adhere to IT-POL-006 standards.

Review Cycle:
As required.

Timeline:
Issued: November 7, 2002

Transition:
Not applicable until product selection.

Procurement:
Until such time that a product standard is selected, agencies must assure that products being considered for purchase comply with the technical specifications listed under Approved Standards. After the product standard is selected, agencies will be required to purchase from the resulting statewide master agreement.

Date: ___________________

Approved by: ________________________________